ABSTRACT OF THE DISCLOSURE

A method and system for controlling access to selected resources in a computer system. The system includes a processor and a device coupled to the processor. The device includes one or more sub-devices and one or more access locks. The access locks are configured to prevent access to the sub-devices when the access locks are engaged. The device may include a bridge. The sub-devices may include a duration timer, mailbox RAM, locks for a storage device, overrides for the locks for the storage device, a TCO counter, a monotonic counter, scratchpad RAM, and/or a random number generator. The method includes unlocking security hardware and accessing a first device. The method also includes locking the security hardware and calling an SMM exit routine.